

In this and all subsequent tutorials, questions and parts marked with an asterisk are intended for MATH2988 students only.

Tutorial 1

1. In each case find the greatest common divisor of a and b , and integers r, s such that $\gcd(a, b) = ra + sb$.
 - (i) $a = 14, b = 35$;
 - (ii) $a = 168, b = 132$;
 - (iii) $a = 847, b = 510$.
2.
 - (i) Use Fermat's factorization method to factorize 629 and 3139.
 - *(ii) Let $n = 10875593$. Aiming to factorize n , I found (with the assistance of MAGMA) that $3306^2 - n = 11 \cdot 17^3$ and $3834^2 - n = 11^3 \cdot 13^2 \cdot 17$. Deduce from this that $(3306 \cdot 3834)^2 - (11^2 \cdot 13 \cdot 17^2)^2$ is divisible by n . Now use a calculator and the Euclidean Algorithm to find a factor of n . What is the smallest a such that $a^2 - n$ is a square?
3. Expand out the product $(x^2 - 2xy + 2y^2)(x^2 + 2xy + 2y^2)$. Use the result to determine all pairs of integers n, m such that $n^4 + 4m^4$ is prime.
4. Let n be a positive integer. The number $n!$ (called " n factorial") is defined to be the product of all the positive integers from 1 to n .
 - (i) Show that if n is composite then $(n - 1)!$ is a multiple of n , unless $n = 4$.
 - (ii) Show that if n is composite then $(n - 1)! + 1$ is not a multiple of n .
 - (iii) Compute $(p - 1)! + 1$ for the first five prime numbers p , and check that in each case $(p - 1)! + 1$ is a multiple of p .
 - *(iv) Prove that $(p - 1)! + 1$ is a multiple of p if and only if p is prime.
5. Let k be a positive integer and p a prime, and put $n = p^k$. Find a formula for the sum of all the positive integers that are divisors of n . (Hint: the divisors form a geometric progression.)
- *6.
 - (i) Use the formula $1 + x^k + x^{2k} + \dots + x^{(n-1)k} = \frac{x^{nk} - 1}{x^k - 1}$ to show that if b divides a then $2^b - 1$ divides $2^a - 1$.
 - (ii) Suppose that $a = qb + r$. Show that $(2^a - 1) - (2^r - 1)$ is a multiple of $2^b - 1$, and hence show that if r is the residue of a modulo b then $2^r - 1$ is the residue of $2^a - 1$ modulo $2^b - 1$.
 - (iii) Let $a, b, n \in \mathbb{Z}^+$, and let $d = \gcd(a, b)$. Use the Euclidean Algorithm to show that $\gcd(2^a - 1, 2^b - 1) = 2^d - 1$.